**Tema** – **“Anatomia de um ataque complexo”** – **Youtube**: <https://www.youtube.com/watch?v=TWX0m8bdwqQ>

1. **Vulnerabilidades(s):**

* Dispositivos IoT com senhas fracas ou padrão: No vídeo, fica claro que muitos aparelhos IoT ainda são instalados com senhas padrão, como "admin" ou "12345". Isso é uma vulnerabilidade crítica, pois essas credenciais são públicas e podem ser facilmente usadas em ataques.
* A ausência de atualização regular de firmware é outra vulnerabilidade mencionada, a qual pode deixar os dispositivos vulneráveis a vulnerabilidades conhecidas, mesmo que já tenham sido corrigidas em versões mais recentes.
* Dispositivos IoT frequentemente não possuem configurações de segurança avançadas ativadas por padrão. Isso inclui a falta de criptografia adequada de dados transmitidos e a falta de autenticação multifator, o que facilita o acesso por atacantes.

1. **Tipos e técnicas de ataque utilizados:**

* Ataque de Força Bruta: No vídeo, o invasor tenta várias combinações de nomes de usuário e senhas em dispositivos IoT para obter acesso. Esse método, conhecido como força bruta, é um dos mais populares e eficazes contra dispositivos que usam credenciais fracas ou padrões fracos.
* Botnets IoT: Uma vez que o dispositivo está comprometido, o atacante pode usá-lo para criar uma botnet, que é uma rede de dispositivos "zumbis" controlados de forma remota. Muitas vezes, essas botnets são empregadas em ataques DDoS (negação de serviço distribuída), nos quais milhares de dispositivos enviam tráfego intenso a um servidor ou site, o que o sobrecarrega e torna inabilitado.
* Man-in-the-Middle (MITM): A comunicação entre os dispositivos IoT e os servidores, muitas vezes, não é criptografada, o que a torna vulnerável a ataques MITM, onde um invasor intercepta e manipula os dados enviados entre o dispositivo e o servidor.

1. **Motivação do cracker:**

* Motivação do cracker.A motivação do atacante pode ser financeira. Ao danificar dispositivos IoT, o hacker pode utilizar essas botnets para realizar ataques de DDoS contra empresas, oferecendo-lhes uma quantia em troca de cessar o ataque. Além do mais, alguns crackers vendem o acesso a redes de botnets no mercado negro.
* Outro motivo para o uso desses dispositivos é a mineração de criptomoedas. Ao comprometer dispositivos IoT que têm capacidade de processamento e deixá-los em segundo plano, o atacante pode utilizá-los para criar criptomoedas, obtendo lucro sem os custos de hardware e energia associados.
* A motivação pode ser alcançar notoriedade na comunidade de hacker em determinadas circunstâncias. Comprometer uma grande quantidade de dispositivos ou fazer ataques massivos pode aumentar o prestígio do cracker em fóruns clandestinos e redes sociais de hackers.